CONFIGURATION MIGRATION UTILITY

FortiConverter™ 4.1

Release Note

FortiConverter™ 4.1 Release Note

July 29, 2013

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document shows how to install and use FortiConverter™ 4.1.

FortiConverter is designed to make it easy to migrate your network to Fortinet network security solutions, significantly reducing workload and minimizing errors. FortiConverter translates configuration files from other vendors' firewall products into a valid FortiGate configuration file. Because the output uses command line syntax, it can either be uploaded as a configuration file or piped to the CLI.

For additional documentation, please visit:

http://help.fortinet.com/fconverter.html

Supported vendors & configuration objects

FortiConverter can translate the following configurations from the following platforms.

Some parts of the configuration may not be machine translatable due to dependencies or syntax that do not exactly correspond. If so, you must manually convert these parts, deciding how your new system will behave.

Vendor	Models	Versions	Convertible Objects
Check Point	Smart Center	NG FP1 (4.) to NGX R64/R71/R75	Interfaces (Physical, Logical, Loopback, PPPoE) Addresses & Address Groups Static Routes Services & Service Groups Schedules Rules NAT (Automatic & Rule) VPN (IPSec) Local Users & Groups RADIUS, TACACS+, & LDAP
Cisco	PIX ASA FWSM	4.x to 8.x	Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) Addresses & Address Groups

	IOS	10.x to 12.x 15.x	DHCP Servers Static Routes Services & Service Groups Time Ranges ACLs NAT IP Pools VPN (IPSec, PPTP/L2TP) Local Users & Groups RADIUS, TACACS+, & LDAP
Juniper	SSG	ScreenOS/JunOS 5.x to 6.x	Interfaces (Physical, Logical, Loopback, PPPoE, Tunnel) Zone Addresses & Address Groups & FQDNs DHCP Servers & Client & Relay Static Routes Services & Service Groups Policies VIPs/MIPs NAT IP Pools VPN (IPSec, PPTP/L2TP) Local Users & Groups RADIUS & LDAP
SonicWALL	NSA Serials	SonicOS Enhanced 5.x	Interfaces (Physical, Logical, Loopback, PPPoE) Zone Addresses & Address Groups & FQDNs DHCP Servers & Client & Relay Static Routes Services & Service Groups Schedules Policies NAT Local Users & Groups

Licensing

Without license activation, FortiConverter functionality will be limited by a trial license: SonicWall conversion will not be supported, fine-tuning will not be available, and conversion will be limited to 100 policies.

After you have purchased and uploaded your license, FortiConverter will be unlocked. Your license entitles you to all new versions of FortiConverter that are released until the license expires.

System requirements

To install FortiConverter, you must have a computer with one of the following operating systems:

- Microsoft Windows 8 (32-bit or 64-bit)
- Microsoft Windows 7 (32-bit or 64-bit)
- Microsoft Windows Vista (32-bit or 64-bit)
- Microsoft Windows XP (32-bit)

Your computer also must have .NET Framework 4.0 installed. If it does not, the installer will prompt you to download and install it first.

Enabling visual effects (Aero) in Windows 7 or Windows 8

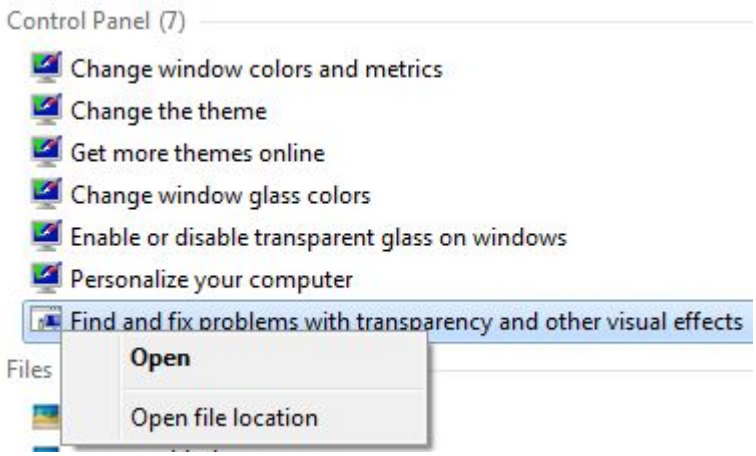
Without Windows Aero Glass Transparency effect, the many premium user interface (UI) goodies and extravaganza visual experience such as windows with translucent glass design and new windows colors in Windows 7 won't be enjoyed by the system users.

To display Aero effects such as transparency in Windows 7

1. Calculate your Windows Experience Index to verify that your computer's hardware is capable of supporting the visual effects..
2. Click the Start Menu to open it
3. Type the following text into the Start Menu search box:

   `Aero`

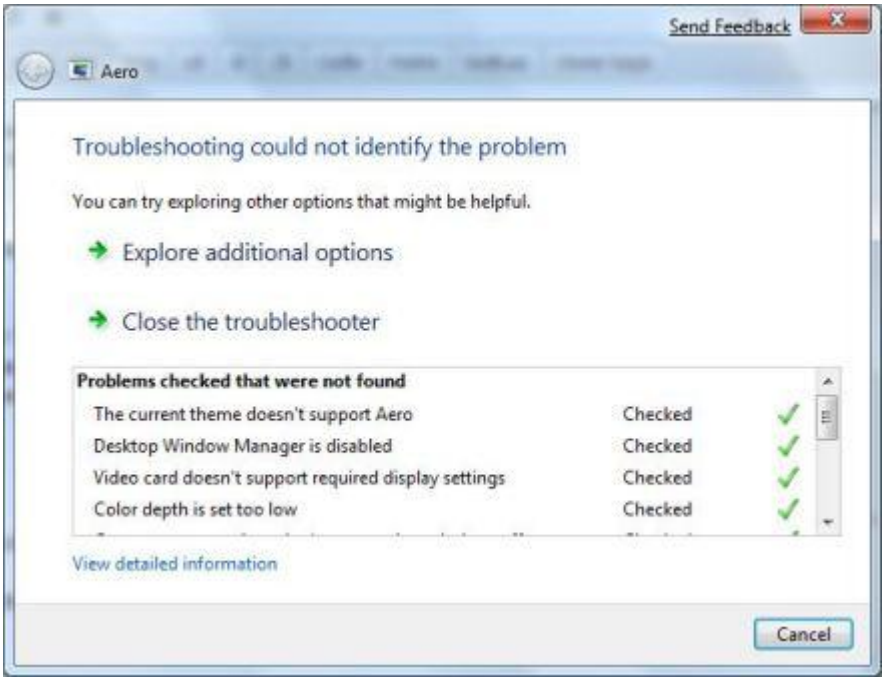
4. In the Control Panel group, click *Find and fix problems with transparency and other visual effects*.



If that option does not appear in the search results, click *Control Panel* to see all Aero-related items in the Control Panel.

5. An *Aero – Troubleshoot computer problems* wizard dialog will appear. Click *Next*.
6. The troubleshooting wizard will try to detect any problem in various components required by Aero, such as video memory, the Desktop Windows Manager (DWM) service, color depth, theme, power settings, etc. When the analysis is complete, the wizard will attempt to fix the issues, then restart Aero.

   If there is still items that are marked with a red X (problems that prevent Aero from functioning properly), fix the issues, then rerun the *Find and fix problems with transparency*



and other visual effects troubleshooting wizard again.

What's new

- Ability to manually fine-tune before you generate output
- Logging
- Support for conversion from these platforms:
  - FortiOS 5.0
  - Juniper ScreenOS 6.x
  - Cisco IOS 15.x
- Support for host names
- For migrations from Check Point, support added for firewall rules, NAT rules, static NAT objects, and hide NAT objects filtered by user-assigned firewalls
- For migrations from Cisco:
  - Support for DNS
  - Support for VLAN reorganization on FWSM
  - Support for commands such as `nat(inside) 0...` (no source NAT) and `static (inside, VPN) 203.0.234.0 203.0.234.0 netmask 255.255.255.0` (mandatory static NAT) on PIX
  - Support for source NAT with IP pools (multiple possible translations) on PIX
  - Support for access lists with more than two `object-group` keywords
  - Support static/source NAT with the `access-list` keyword on ASA/IOS
- For migrations from Juniper ScreenOS:
  - Support for VIPs without an IP
  - Support for DNS

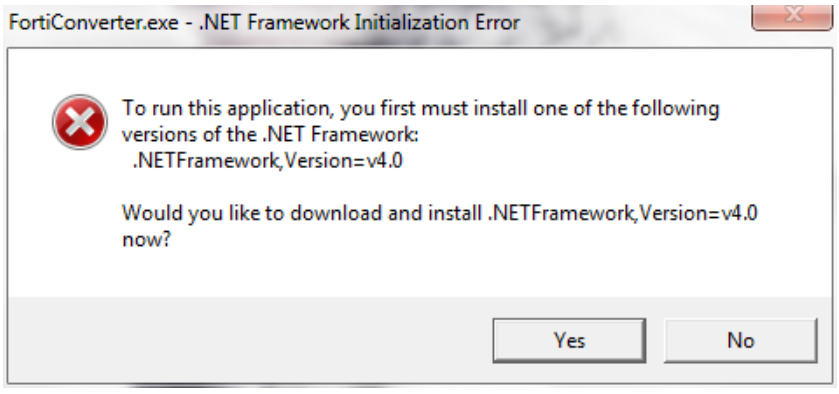
Installation

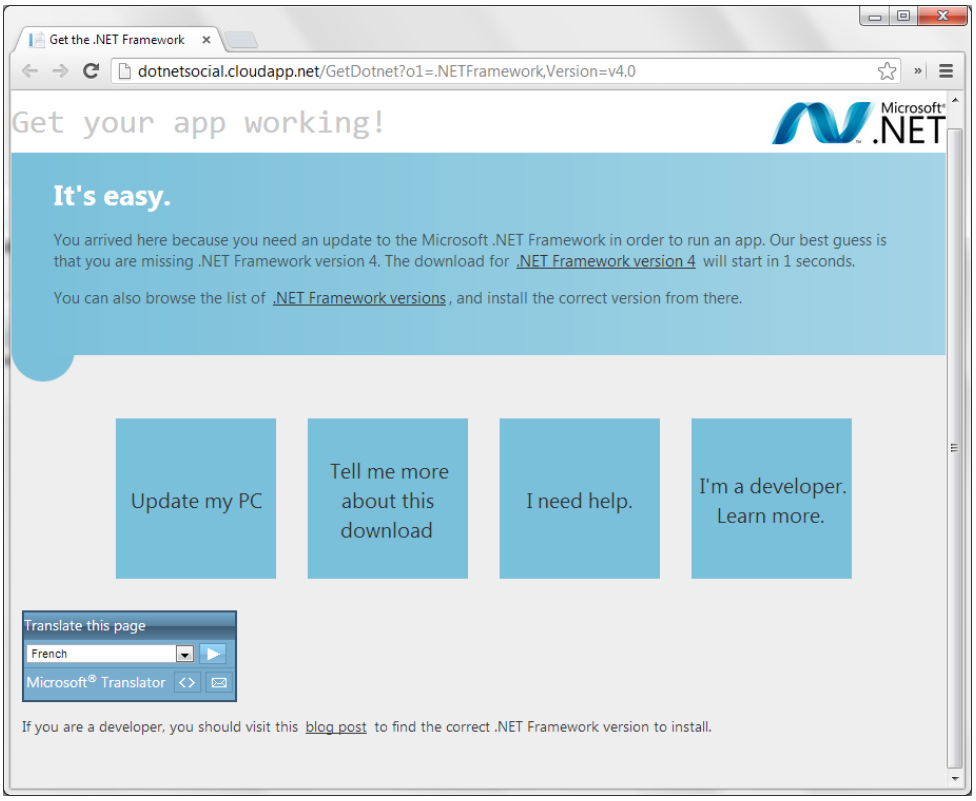
You can download the FortiConverter installer from Fortinet Technical Support's web site, https://support.fortinet.com .

To install FortiConverter

7. Double-click the FortiConverter installer executable (.exe).

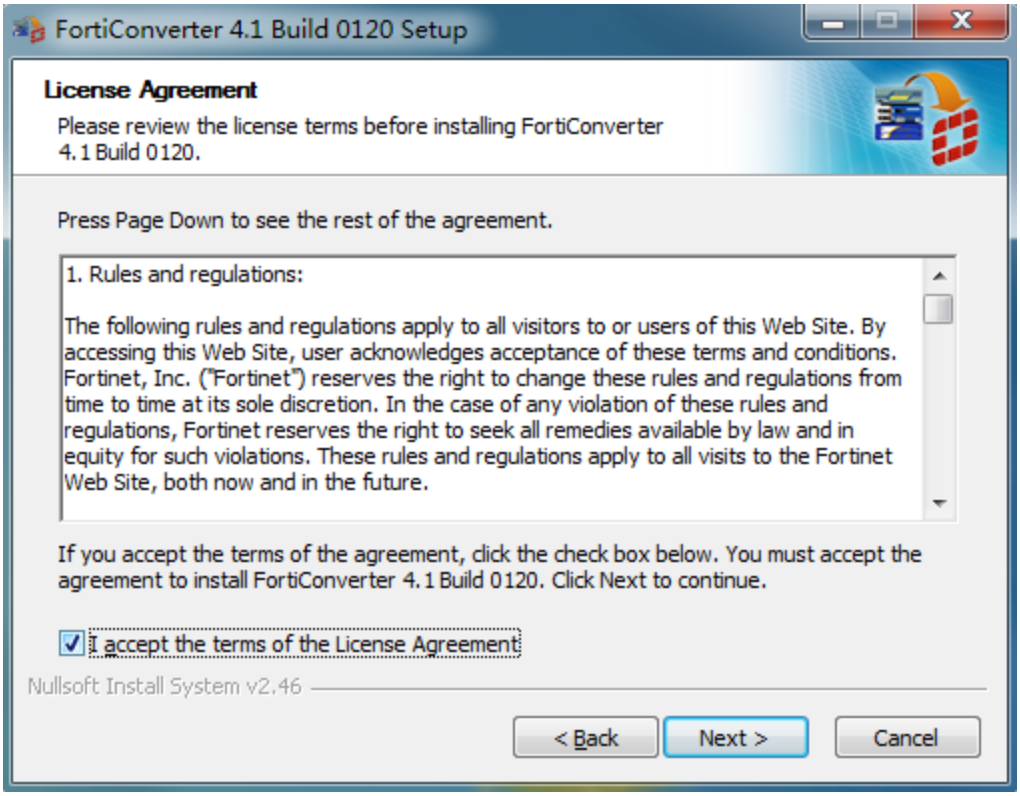
   If your computer does not have the required Microsoft .NET Framework 4.0, you will be prompted to install it before the installer will launch.



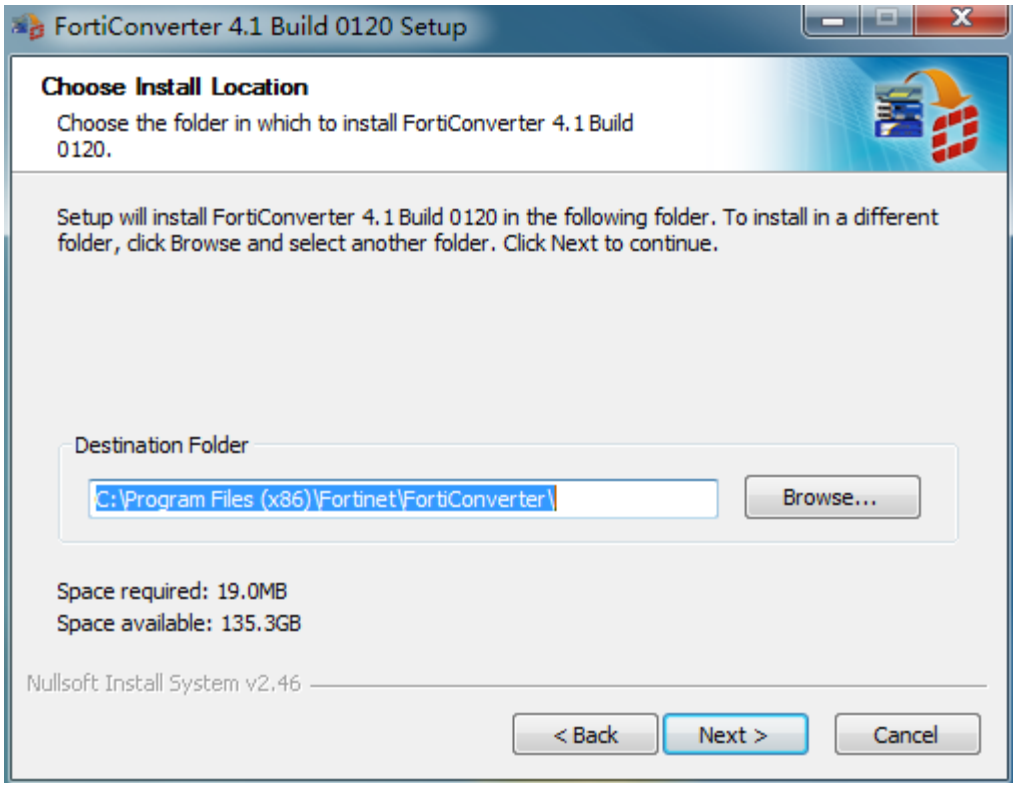


Otherwise, the beginning of the installer should appear.

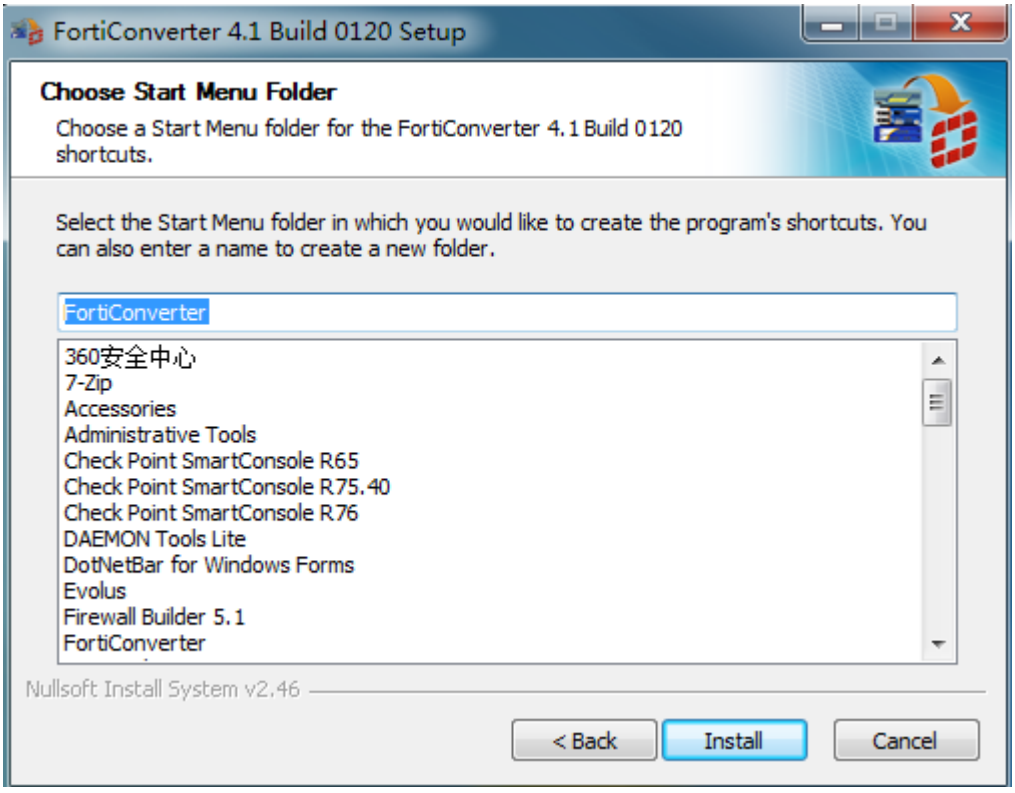
8. Read the license agreement. If you agree to the terms, mark the *I accept the terms of the License Agreement* check box, then click *Next*.



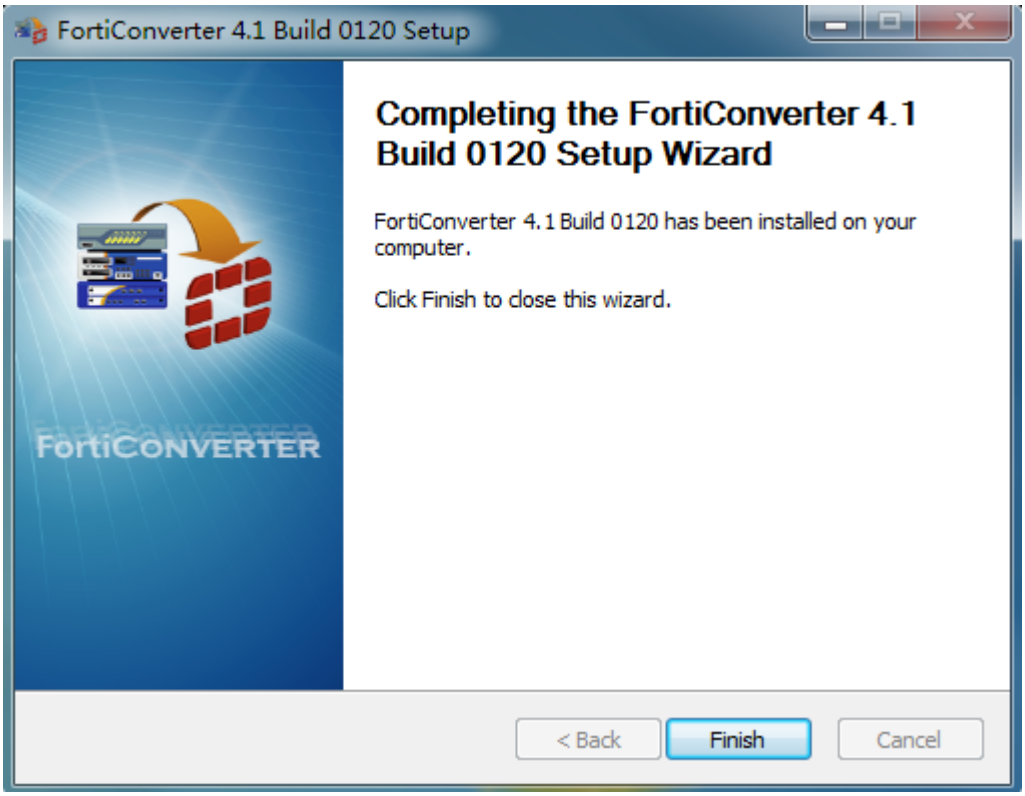
9. If you want to install in a different location, click *Browse* and select the directory. Otherwise, click *Next*.



10. Select the *Start Menu* folder in which you would like to create the program's shortcuts, then click *Install*.



11. Click *Finish* to exit the FortiConverter installer.



Uploading the license

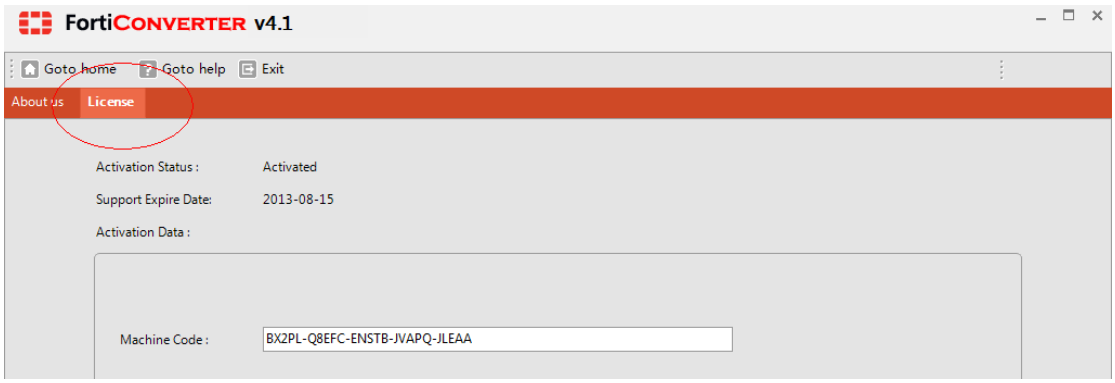
After installation, FortiConverter initially has a temporary, restricted trial license. If you have purchased an unrestricted, permanent license, upload it to unlock additional capabilities.

To activate the license

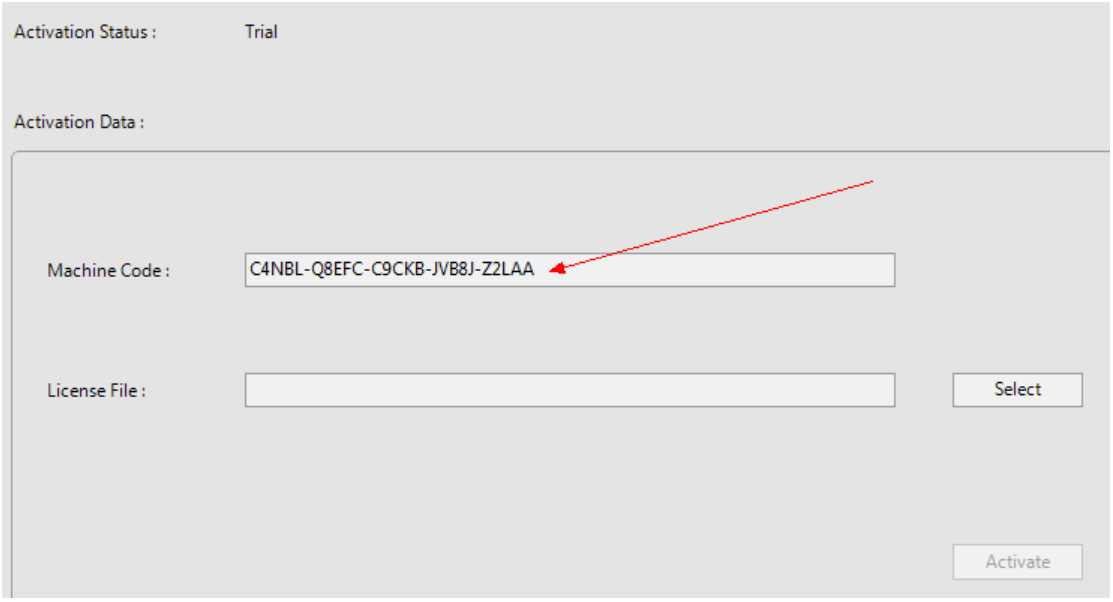
1. Start FortiConverter.

2. Click the *System Setting* square.

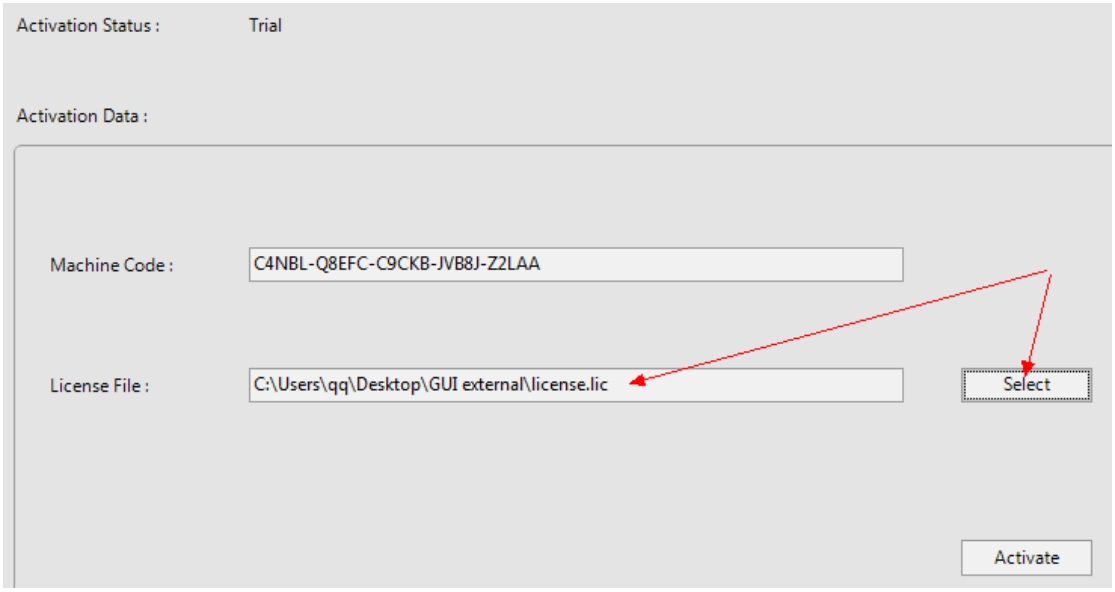
3. Click the the *License* tab.



4. Copy the contents of the *Machine Code* field.

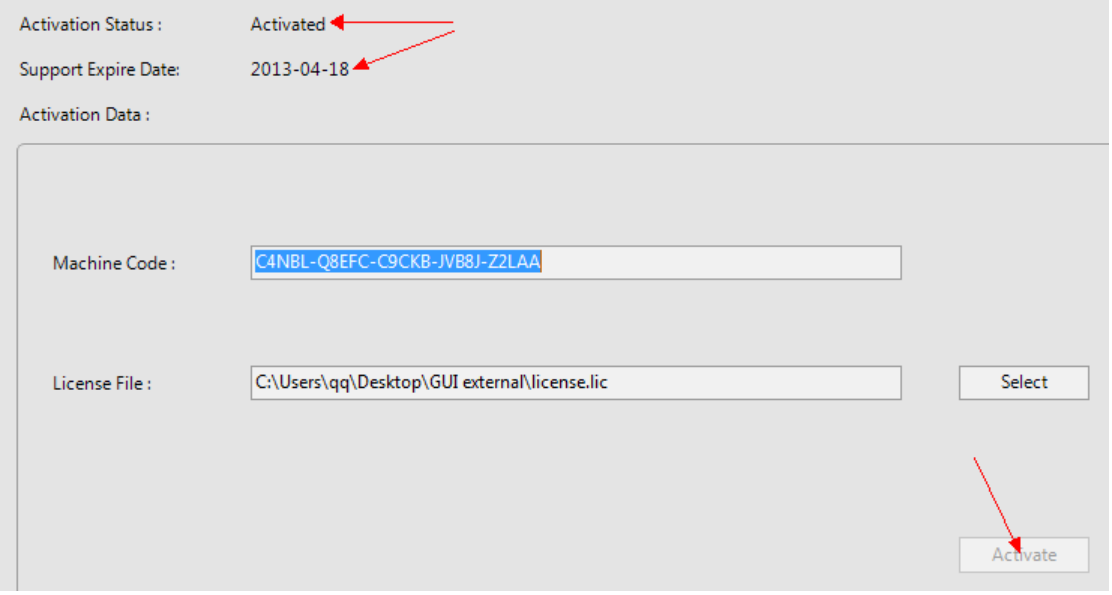


5. Start a web browser and go to the Fortinet Technical Support web site:
   https://support.fortinet.com/
   Enter your machine code to activate and download your FortiConverter license (.lic file).



6. Return to FortiConverter. Click the *Select* button to locate the .lic file, then click *Activate*.

FortiConverter will validate the license file. If it is valid, *Activation Status* will change from *Trial* to *Activated*. Your license will be valid for all FortiConverter software updates released until the date in the *Expire Date* field.



Conversion

After inputting your previous vendor's configuration files, you can fine-tune the conversion before outputting your new FortiGate configuration file.

Downloading configuration files that you want to convert

To use FortiConverter to migrate a configuration from your legacy firewall, you must first download your existing configuration to your computer.

Procedures vary by vendor. Some vendors divide the configuration into multiple files, so be sure to download all files.

Check Point

To get the configuration, you must download 3 or 4 files:

- **Object definitions**— 'objects_5_0.c' (Check Point NG/NGX) or 'objects.c' (Check Point 4.x) contains the firewall's object definitions.
- **Policy and rule definitions**— '*.w' or 'rulebases_5_0.fws' The file name is <rule>.W (default Standard.W). or rulebases_5_0.fws . You can get them from the directory "[SmartCenter]\fw1\conf\".
- **Route information** — Helps FortiConverter to correctly interpret the network topology being converted. To get this data, enter the `route print` command, then copy and paste the output into a plain text file. Codes in the output indicate if it is a directly connected interface, a host route, a network route, and so forth. The output varies by the platform.
- **User and user groups file** — fwauth.NDBx

Cisco

To get the configuration, enter the `show running-config` command, then copy and paste the output into a plain text file.

Juniper

To get the configuration, use either the web UI (go to *Configuration* > *Update* > *ConfigFile*) or CLI (enter the `get conf` command, then copy and paste the output to a plain text file).

SonicWALL

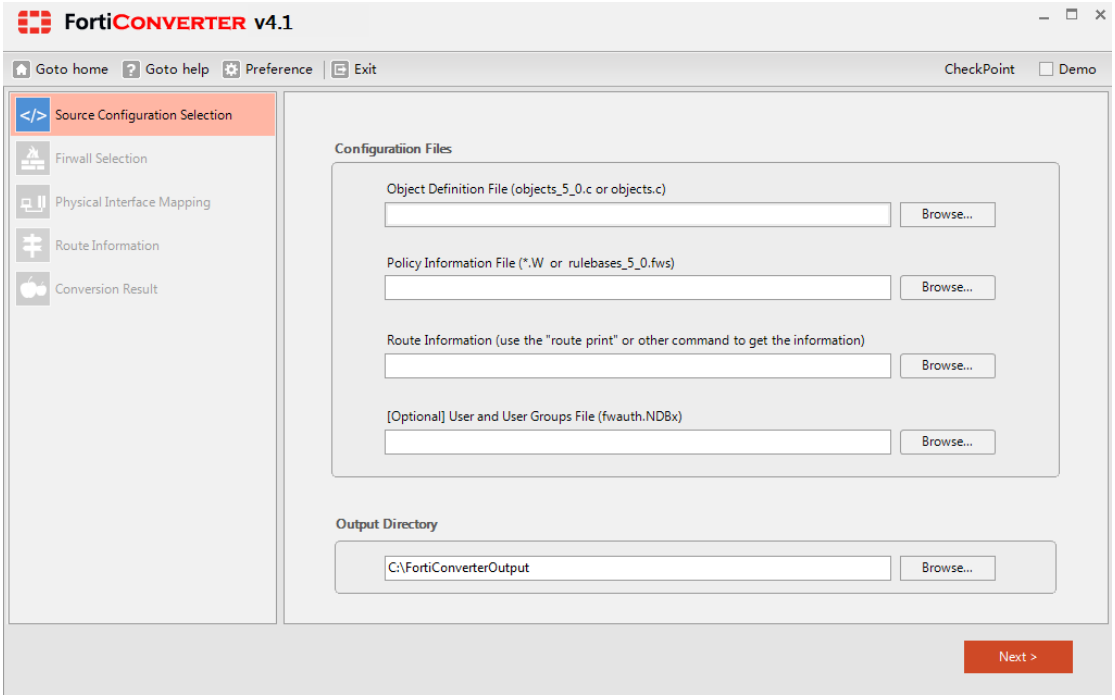
To get the configuration (*.exp file), use the web UI and go to *System* > *Settings* > *Export Settings*.

Using the conversion wizard

FortiConverter provides a wizard for each supported vendor to help you automatically migrate as much as possible of the configuration. At that point, you can optionally manually fine-tune the results before exporting the final FortiGate configuration file.

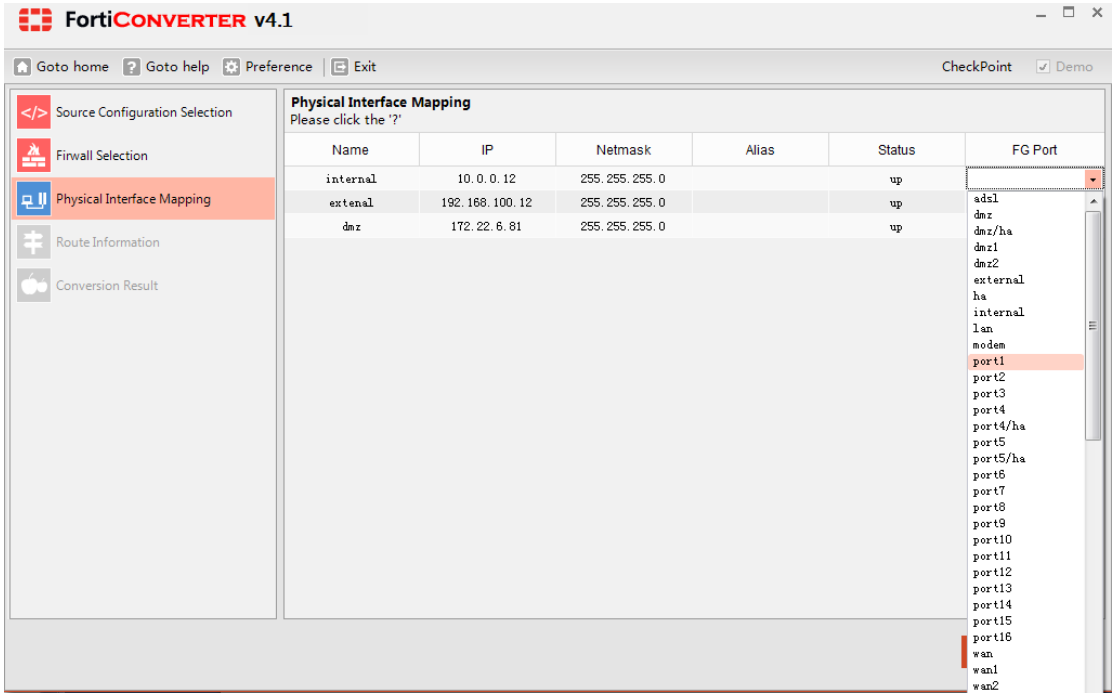
To migrate your configuration

1. Start FortiConverter, then click on your vendor's square.
2. Load your previously downloaded configuration files, then click *Next*.

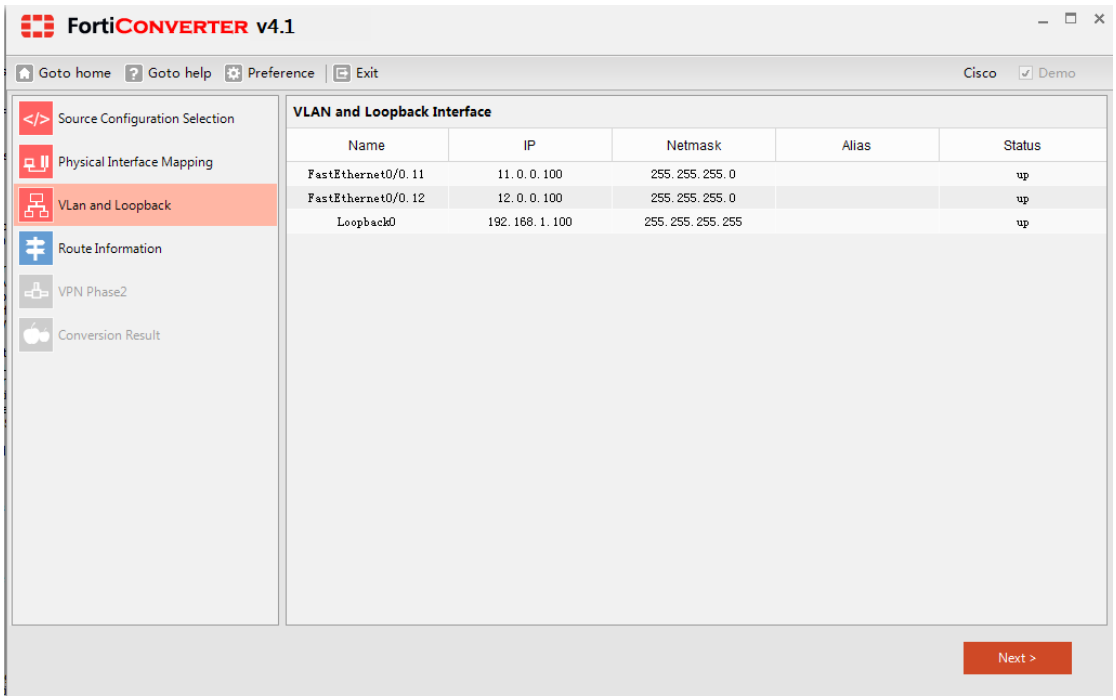


3. If you are migrating from Check Point, select which firewall model that you have. (Check Point may store multiple firewalls in the object definition file.)

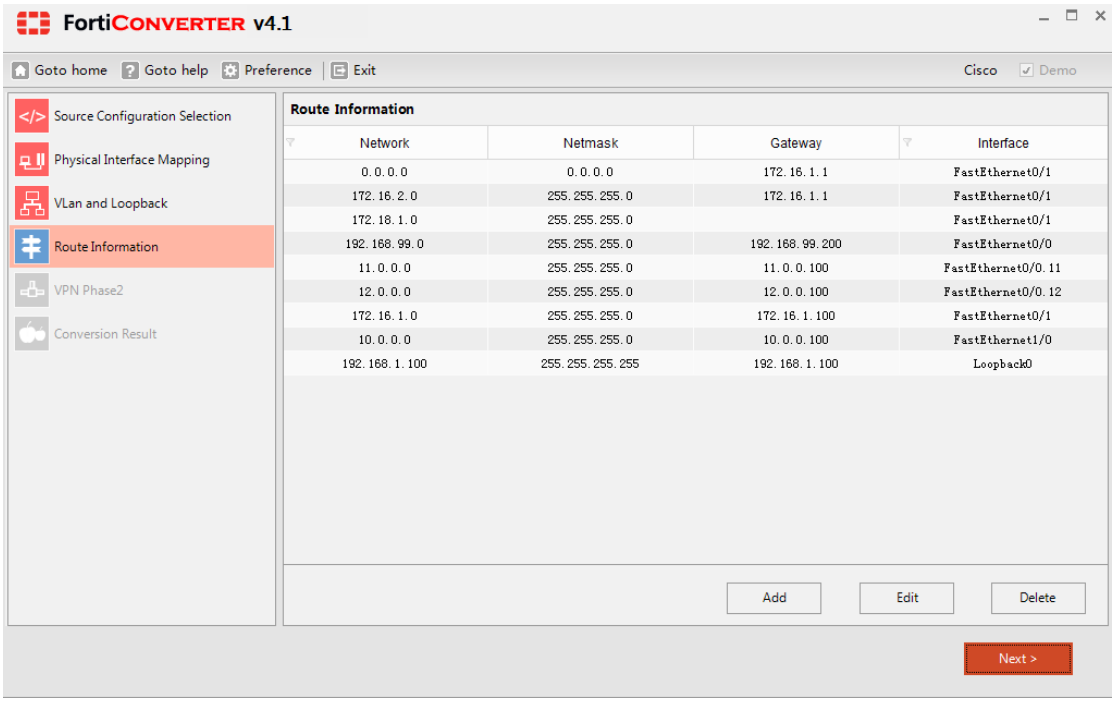
4. Map your network interfaces on Check Point / Cisco / Juniper/ SonicWALL to specify the names they will have on your new FortiGate firewall.



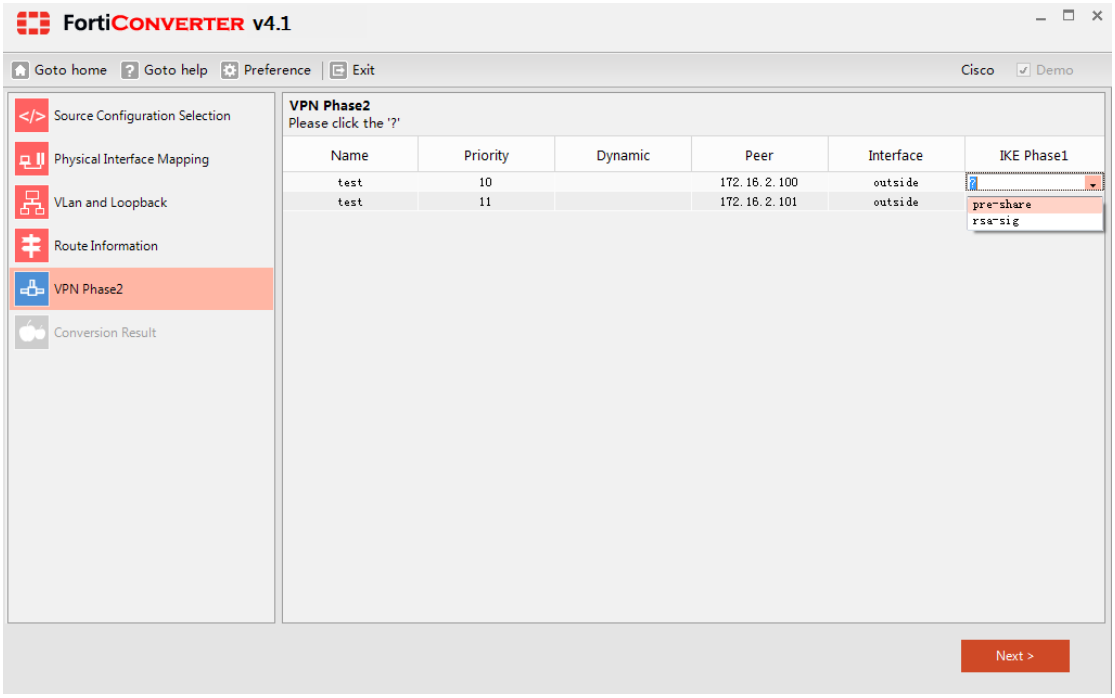
5. If there are logical interfaces such as VLANs or loopback interfaces defined in the configuration that you are converting, verify their conversion.



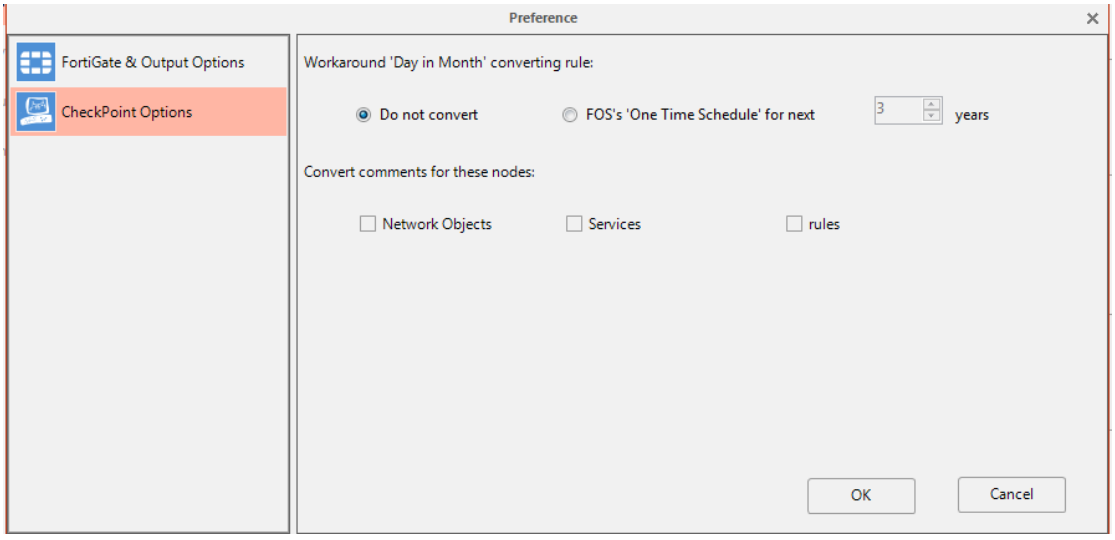
6. To correctly interpret the direction of rules and interface, add routing information. (These routes will not be part of the final configuration.)



7. If you are converting Cisco IPSec Phase 1 and Phase 2 definitions, these cannot be automatically converted. Enter them manually.

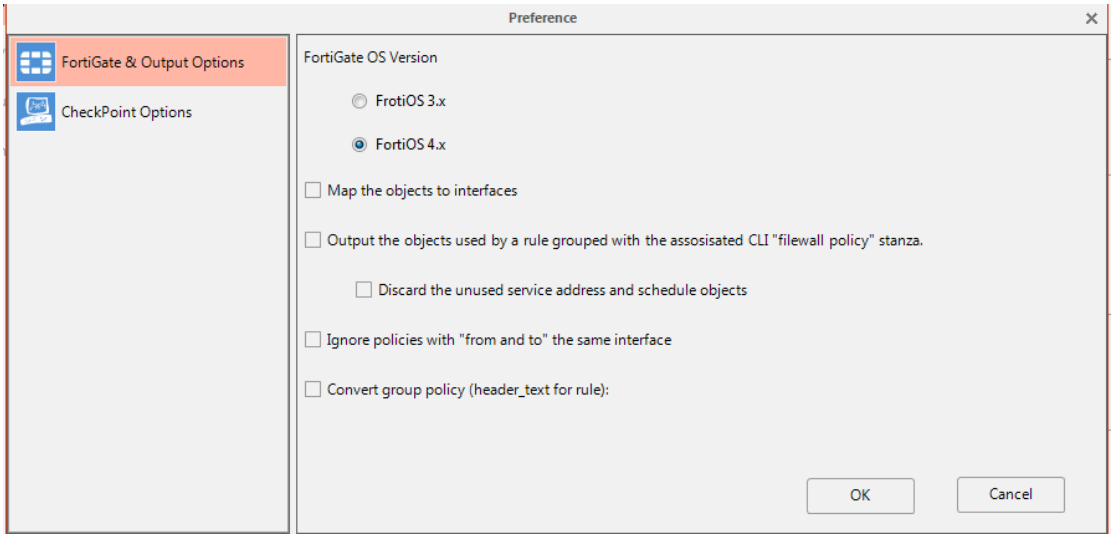


8. Review the results of the conversion.



Preferences

To define preferences, click the *Preference* button on the top toolbar.



If you enable *Map the objects to interface*, FortiConverter will do a reverse-look-up and map address objects to relevant interfaces. If there is any inconsistency, FortiGate will reject the policy. As a result, some policies may be lost when loading converted configurations onto your FortiGate. Please use this function carefully.

For Check Point conversions, there are additional options.

For an optional way of converting Check Point time objects, you can select how to handle the “Day in Month” setting. Check Point firewalls have a time object that specifies days of the month, but this does not exist on FortiGate. Therefore you can choose either ‘Do not convert’ or convert to a number of one-time schedules. FortiConverter will create these one-time schedules for the next three years.

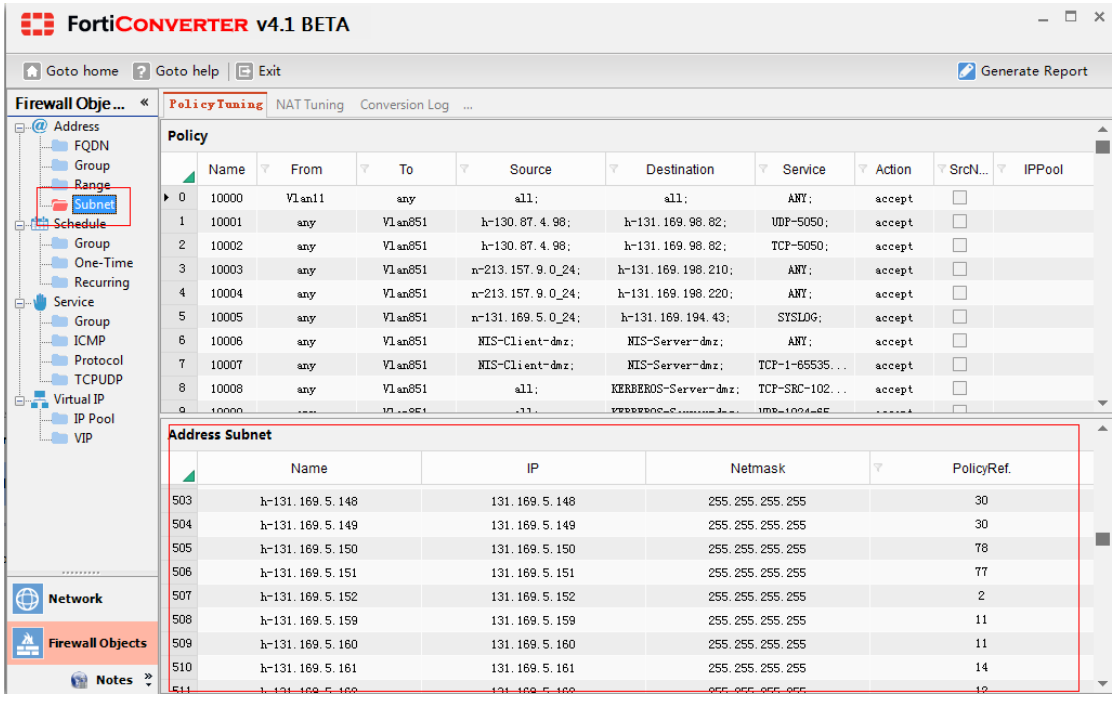
Fine-tuning

Firewall objects

		Show	Edit	Add	Delete	Policy locate
Interface	Interface	√	√	√	√	√
	Zone	√	√	√	√	√
Address	Subnet	√	√	√	√	√
	Range	√	√	√	√	√
	FQDN	√	√	√	√	√
	Group	√	√	√	√	√
Service	TCPUDP	√	√	√	√	√
	ICMP	√	√	√	√	√
	Other	√	√	√	√	√
	Group	√	√	√	√	√
Schedule	Once	√	√	√	√	√
	Recur	√	√	√	√	√
	Group	√	√	√	√	√
NAT	VIP	√	√	√	√	√
	IPPool	√	√	√	√	√

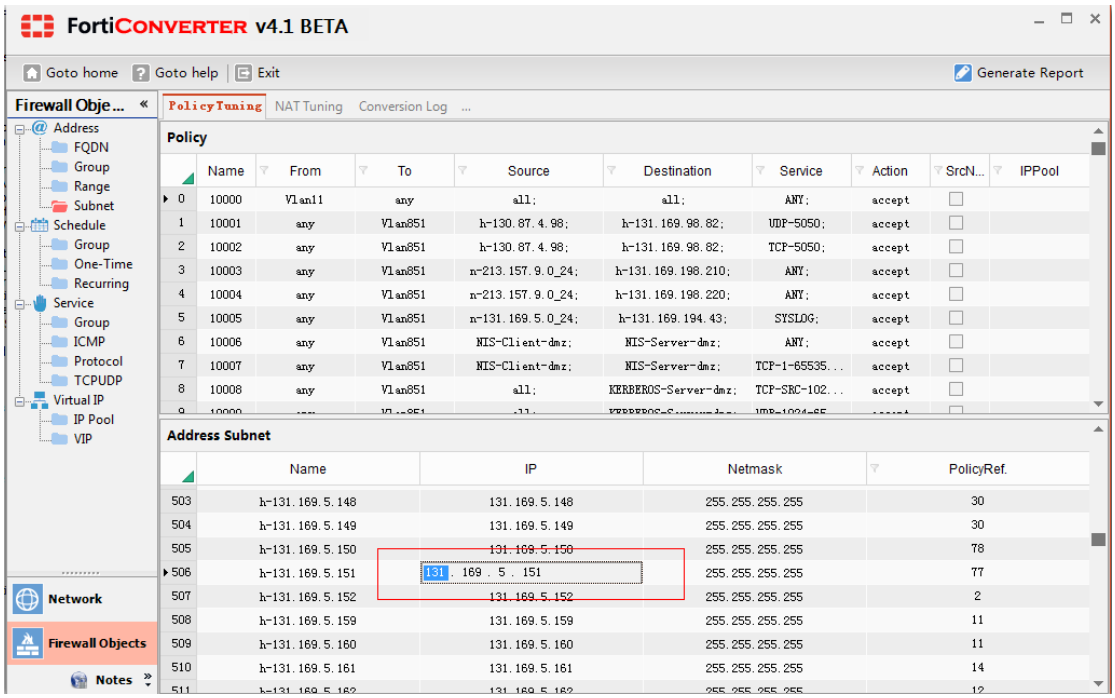
Show

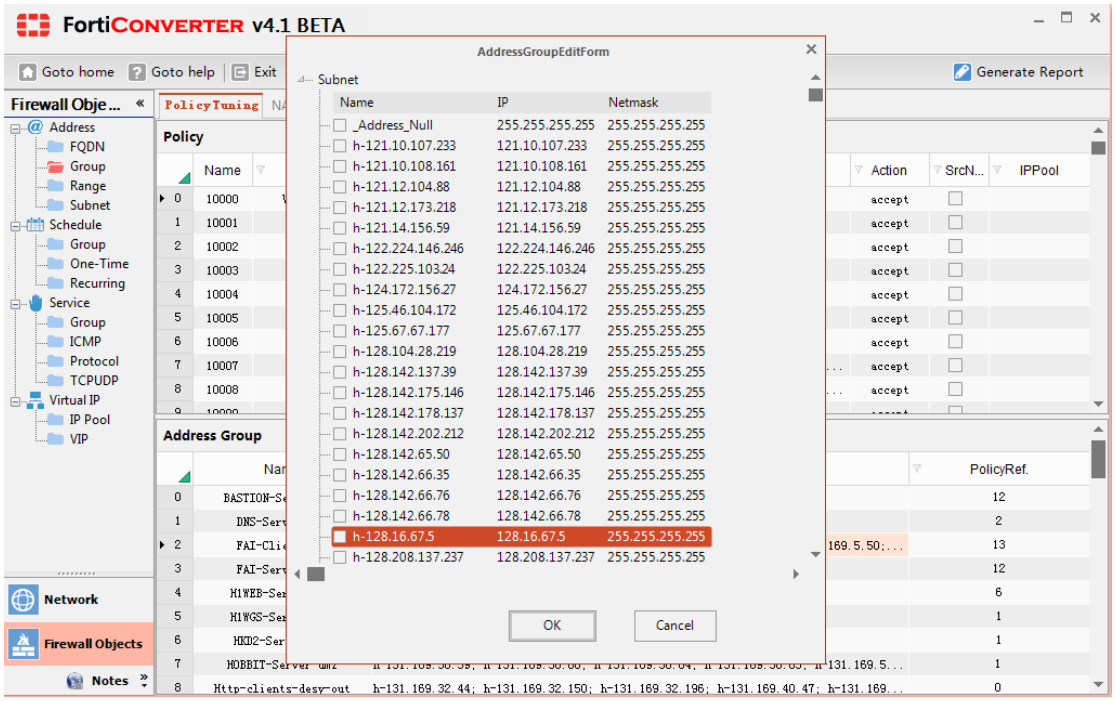
To show an item in the table on the bottom right, click the tree view button of that specific firewall object.



Edit

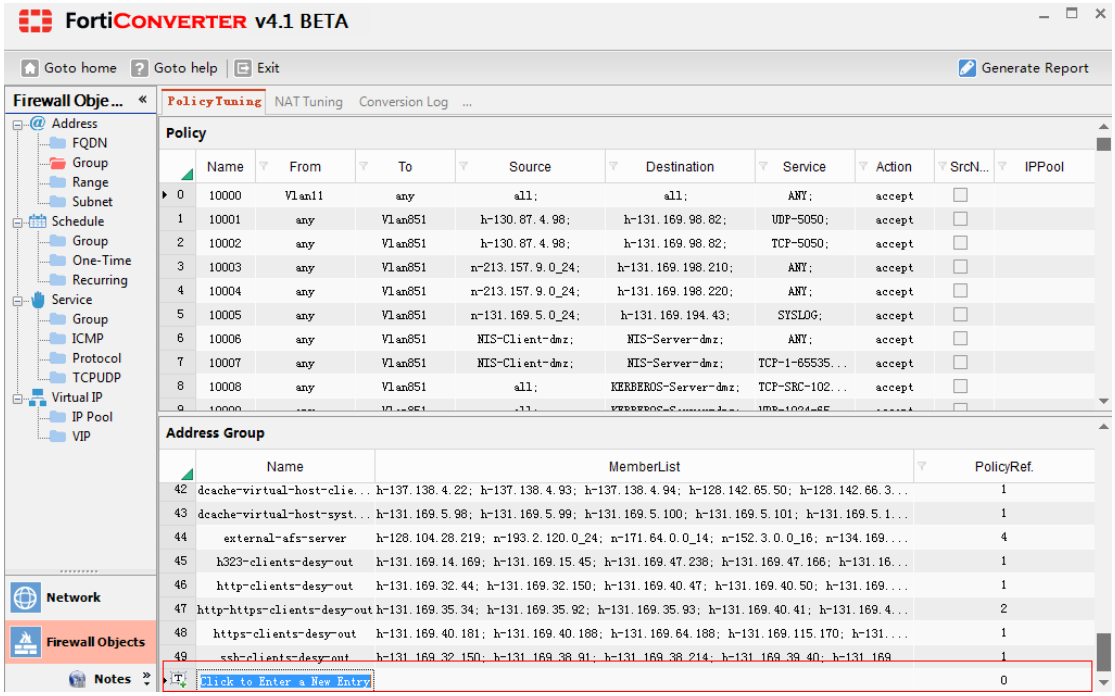
To edit an item, either click its table cell and begin typing, or use the pop-up dialog.





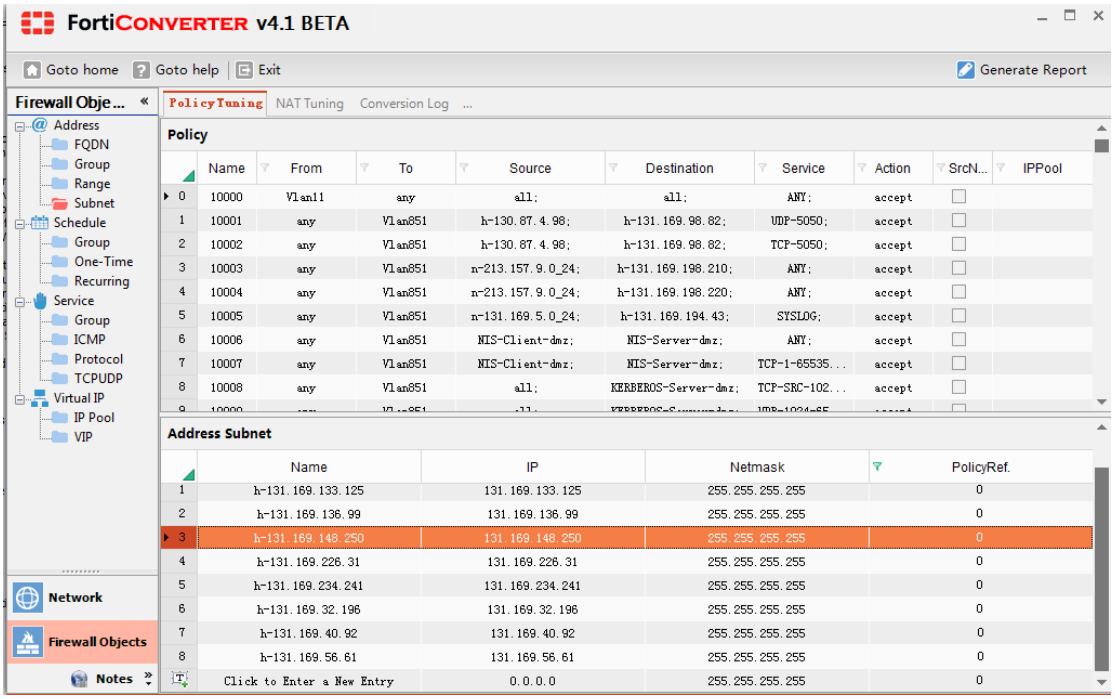
Add

To add a new item, click the bottom row and begin typing.



Delete

To delete a specific line, click the row's index number, then press the Delete key. Note that only items that are not referenced by any policy or group can be deleted.



Policy Locate

The *PolicyRef*. column shows the number of polices that reference that firewall object. By clicking the content, the specific numbers of policies will be shown in the policy table on the top right.

Policy

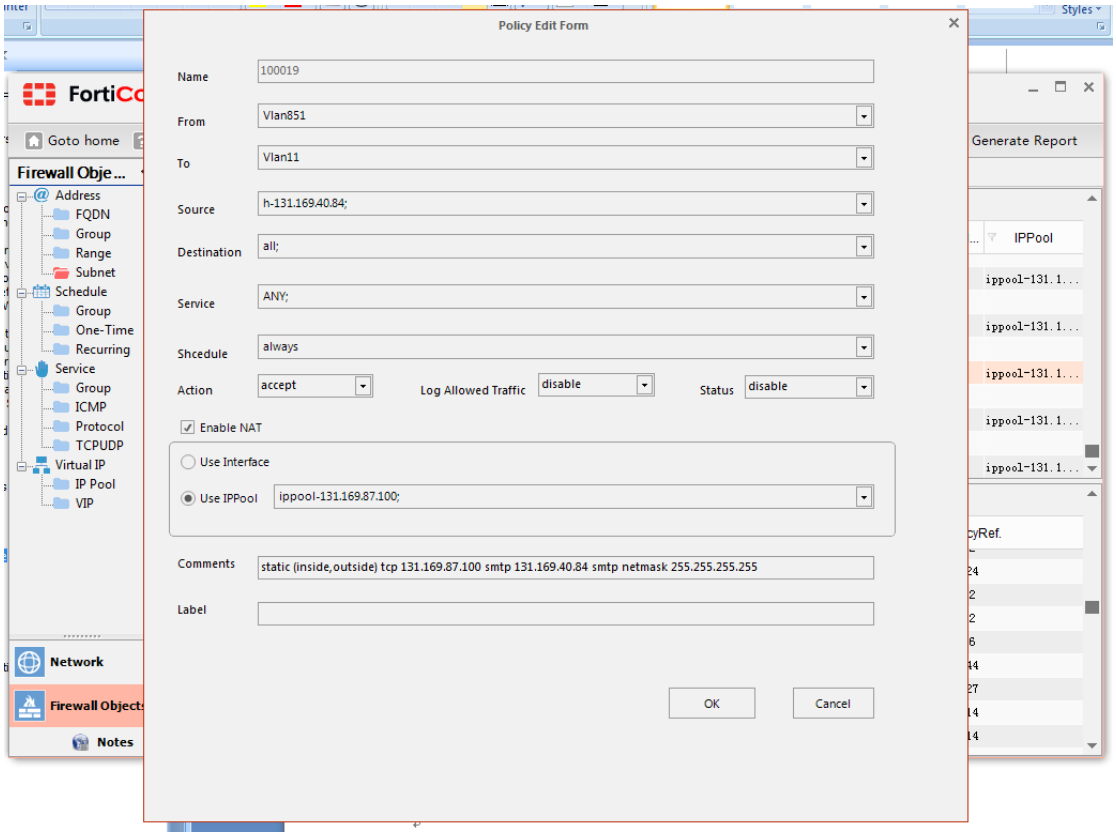
	Show	Edit	Add	Delete	Filter	Reorder	Objects Tooltip
Policy	√	√	√	√	√	√	√

Show

When the fine-tuning form is loaded, the table is initially displayed. Its appearance varies by firewall object policy references. Clicking on any tree view button will cause the policy table to refresh.

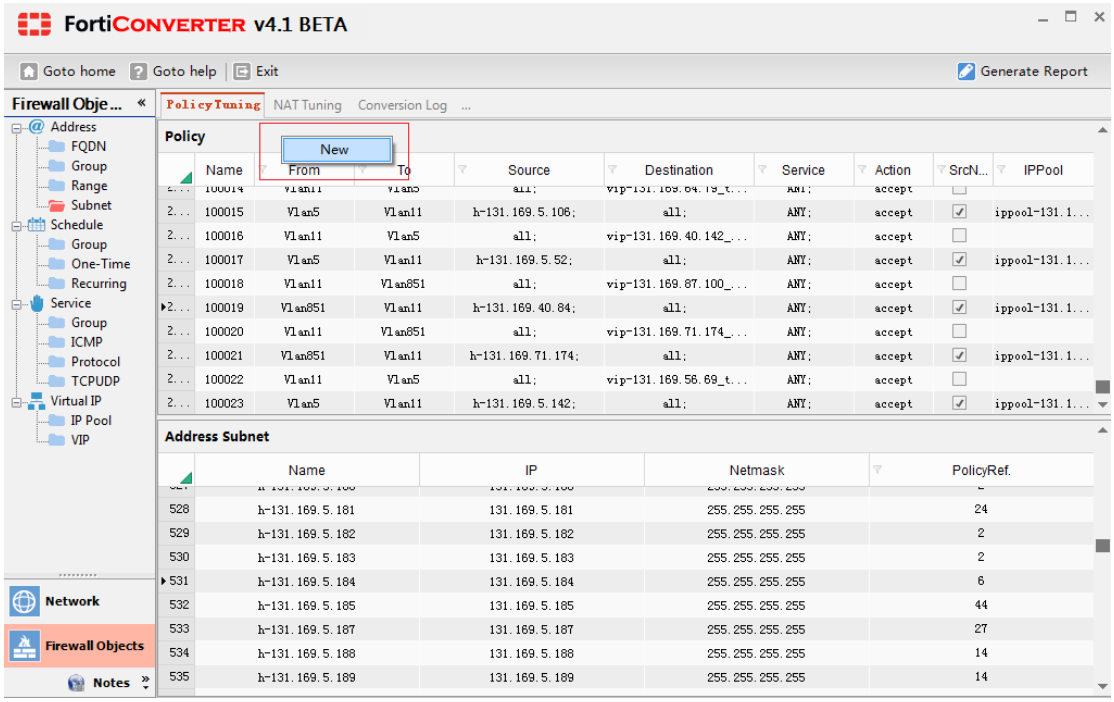
Edit

To edit any cell of the specific policy row, click it and begin typing. Alternatively, you can use the pop-up dialog.



Add

To add an object, right-click, then select *New*.

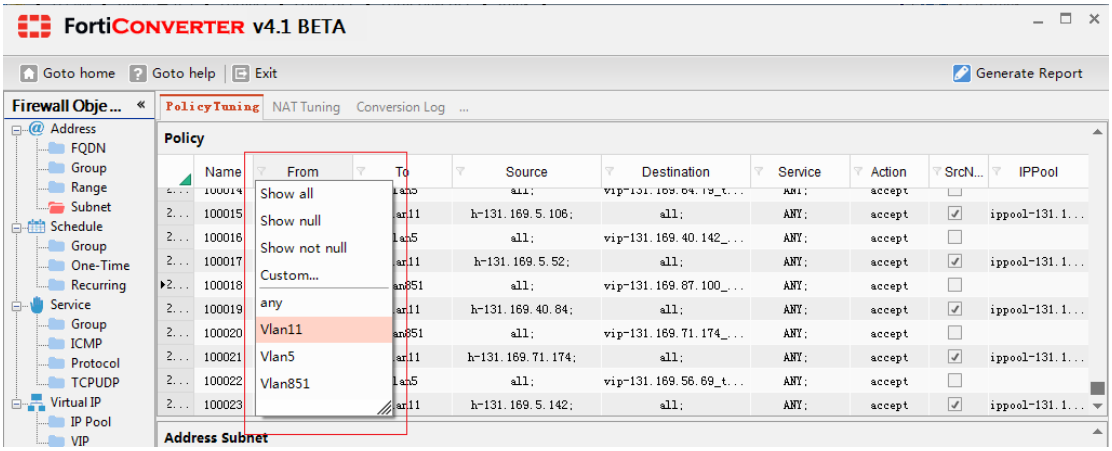


Delete

To delete a line, click its header, then press the Delete key.

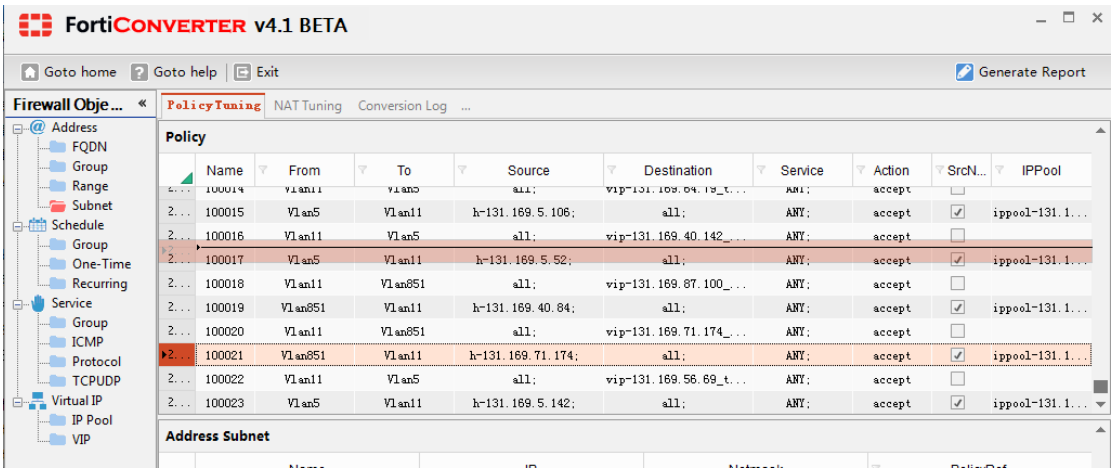
Filter

Every column with the [filter mark] can be filtered by a given option or custom expression.

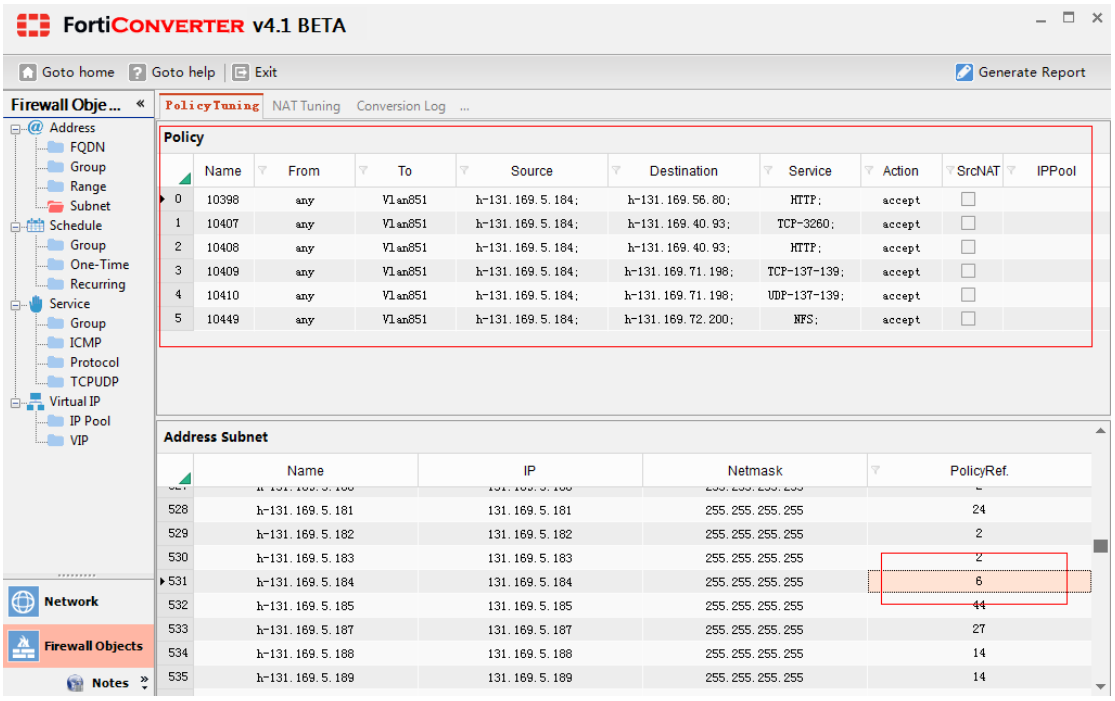


Reordering columns

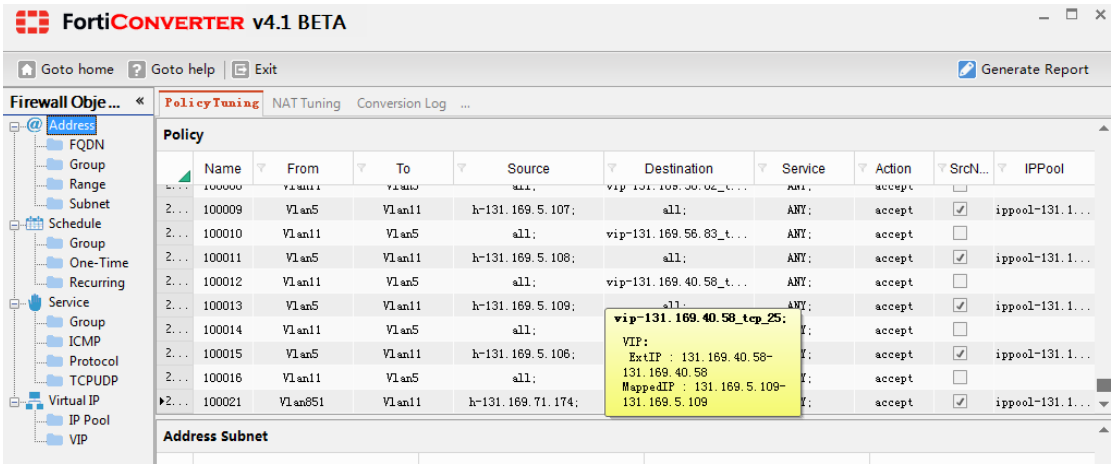
To reorder columns, drag and drop them into position



Object tooltips



Contents of a firewall object will be shown as tooltip when hovering your mouse over the item.



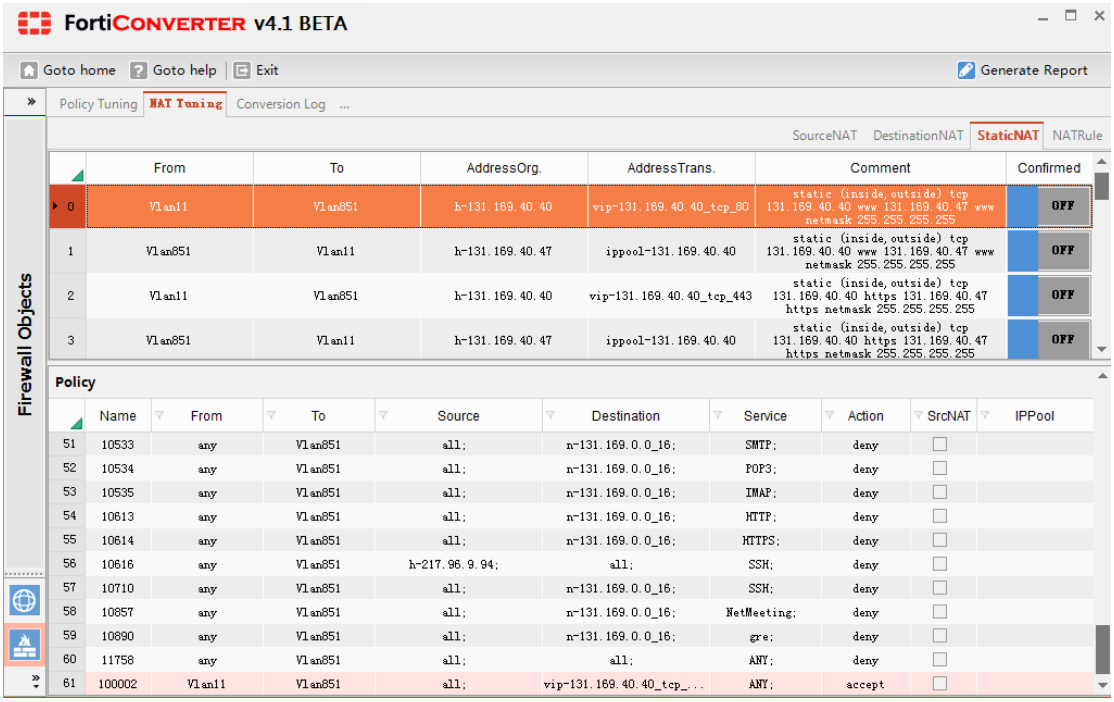
NAT policy

	Show	Policy Locate	Objects Tooltip
SourceNAT	√	√	√
DestinationNAT	√	√	√
StaticNAT	√	√	√
NATRule	√	√	√

You can fine-tune your NAT conversion by clicking the *NAT Tuning* tab. All NAT has been divided into 4 categories: Source NAT, Destination NAT, Static NAT, and NAT Rule.

To select a NAT item, click on the row header. All related policies will be shown on the policy grid table right below with auto-generated ones highlighted with a light red color background.

You can manually adjust and merge inside the policy grid table.



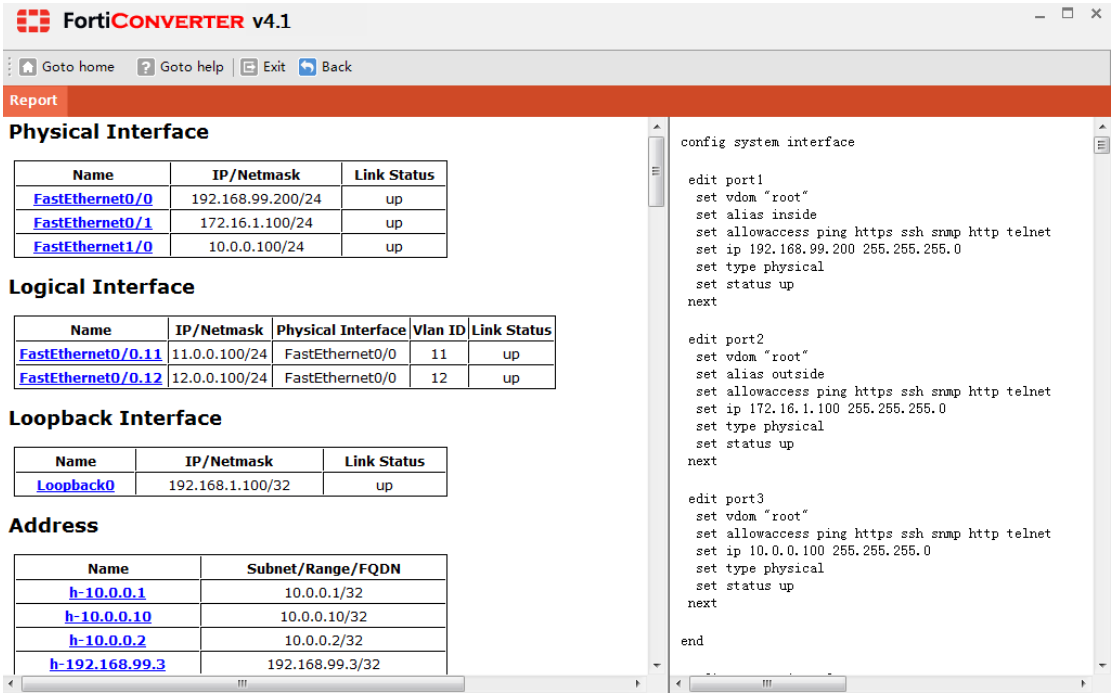
Note:

1. For a Juniper-ScreenOS configuration which already has NAT configured inside a policy, it will be automatically converted. NAT fine-tuning is not required.
2. For some of the cases, where interfaces/addresses and service match completely, NAT will be automatically merged into the policy.

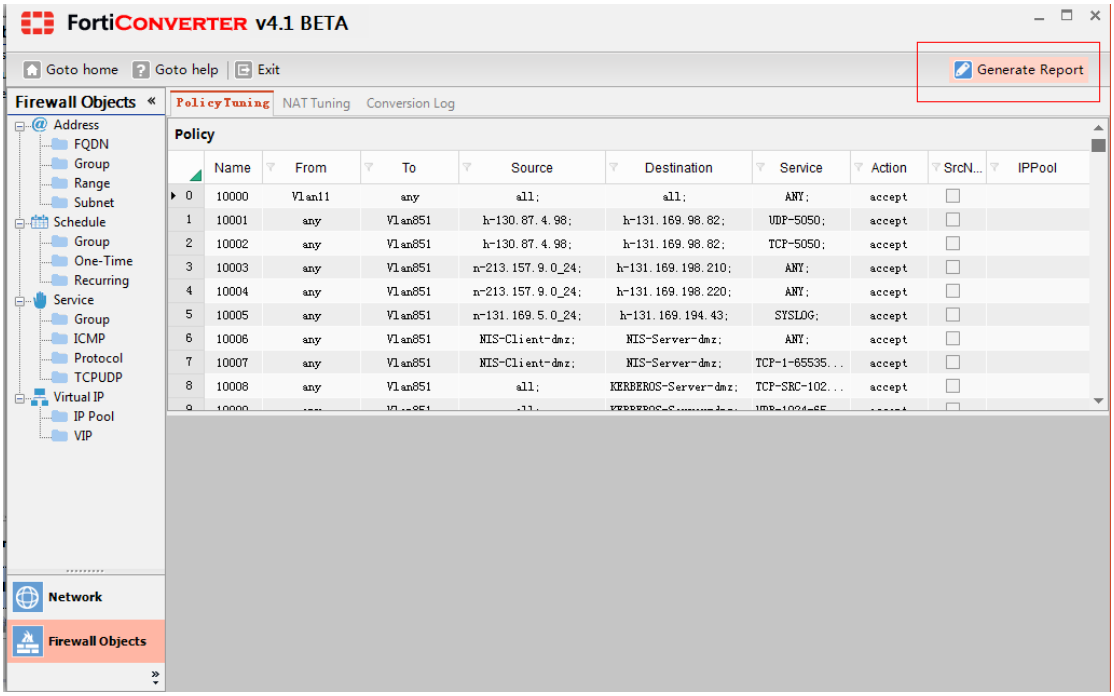
(All Polices with a number starting at 100000 are pure NAT-Polices which must be manually merged, and always placed at the bottom, below all security policies

Report

To see a summary of the conversion report, click *Go to Report*.



Alternatively, click the *Generate Report* button on the fine-tuning form. The configuration will be generated according to your specifications while you were fine-tuning.



Understanding your new configuration

In order to understand your new configuration, familiarize yourself with important differences.

Check Point

- FortiGate's `set allowaccess` command for interfaces does not exist on Check Point. Since this setting is required on FortiGate, FortiConverter will by default enable all services for interfaces.
- The interface "Lead to Internet" is a default static route on FortiGate.
- After converting the VPN configuration, the "Lead to Internet" interface will be referred to for the VPN policy's destination interface.

  If you used the wizard to change the default route's egress interface, you may need to update the VPN/Policy configuration manually.
- "by day in month" time schedules will be converted to FortiGate one-time schedules; "by day in week" and "none" will be converted to a recurring schedules.

  You must assign the year range for the Check Point "by day in month" time object. If the day does not exist for a certain month, FortiConverter will not generate the schedule.

  For example, if you configured the Check Point firewall's "by day in month" time schedule with the below parameters:

  For each year

  ```
  Month: Jan/Match/Sept.
  Day: 1, 5, 31
  Start and end time: 0:00 to 10:00
  ```

  if you had used the FortiConverter wizard to assign year range value 1, and had got current year value 2013 from local PC which run the wizard, the output for FortiGate one-time schedules would be like this:

  ```
  From 0:00 Jan/1/2013 To 10:00 Jan/1/2013
  From 0:00 Jan/5/2013 To 10:00 Jan/5/2013
  From 0:00 Jan/31/2013 To 10:00 Jan/31/2013
  From 0:00 Match/1/2013 To 10:00 Match/1/2013
  From 0:00 Match/5/2013 To 10:00 Match/5/2013
  From 0:00 Match/31/2013 To 10:00 Match/31/2013
  From 0:00 Sept./1/2013 To 10:00 Sept./1/2013
  From 0:00 Sept./5/2013 To 10:00 Sept./5/2013
  ```

  Notice that Sept. 31 does not exist.
- Rule actions with "Client Auth" will be converted to FortiGate user-identity policy with the "Accept" action.
- Static NAT for Check Point is a 1-to-1 IP relationship, but after converting to FortiGate NAT policy, source NAT with an IP pool is not a 1-to-1 relationship.
- On Check Point, VPN is not configured within a firewall rule. When converting to FortiGate, FortiConverter will generate several VPN policies from non-"Lead to Internet" interfaces to the "Lead to Internet" (default route) interface.

Cisco

- FortiGate's `set allowaccess` command for interfaces does not exist on Cisco firewalls. Since this setting is required on FortiGate, FortiConverter will by default enable all services for interfaces
- Cisco `object-group` objects have two types of service definitions. Only `service-object` items can be converted tino FortiGate services because FortiGate services have both a source and destination port. By default, the other type of service object, defined by `port-object`, is not converted. FortiConverter will generate FortiGate service objects from a Cisco ACL's protocol and source/destination port.
- On Cisco IPSec VPNs, Phase 1 (ISAKMP) supports more than two types of authentication methods. FortiGate supports only two types: `pre-share` and `rsa-sig`. Therefore you must assign methods for each VPN connection. Cisco EZVPN configuration will be converted to FortiGate VPN policies from the "Intranet" interface to the interface which was assigned by the `crypto map interface` command.
- FortiConverter does not support Cisco ASA objects for NAT and double NAT.
- FortiConverter does not support Cisco wild card netmasks for `access-list` and `object-group` objects.
- EZVPN conversion is not supported for Cisco IOS.

  For example, `crypto ipsec profile <profile-name>` and `crypto isakmp profile <profile-name>` are not supported.

Juniper

- Interface names starting with "vlan" will be recognized as logical interfaces.

SonicWALL

- On FortiGate '#', '(' and ')' are reserved special characters, and cannot be used in the configuration without a preceding escape sequence. FortiConverter uses these characters to replace them: '*', '[' and ']'. For example, if you have an address book with name "SNWL #1", it will be translated to "SNWL *1". If you have a service book with name "Citrix TCP (Session Reliability)", it will be translated to "Citrix TCP [Session Reliability]".
- On FortiGate, address objects are IP addresses or FQDNs, not MAC addresses. As a result, SonicWALL MAC addresses will not be migrated.
- FortiConverter will generate two extra address book entries: "Any" and "_Address_Null". "Any" is added because it is a default address book in SonicWALL.
  The reason for "_Address_Null" is that FortiGate address groups do not allow an empty group without any members, so "_Address_Null" can only be referred to by empty address groups.

Service book configuration:

- If you have configured a service book/group on SonicWALL, but this is predefined on FortiGate (such as HTTP port 80, HTTPS port 443, etc.), then the object would conflict, and therefore will not be generated.

Schedule configuration:

- SonicWall schedule group configuration has a little difference with FortiGate schedule group; SonicWall schedule group can contain only one "onetime" schedule and multiple

"recur" schedule. The "onetime" schedule is an implicit object which can be embedded to the schedule group. But FortiGate cannot support this implicit attribution, every object (onetime or recur) which can be referred by schedule group need to be defined explicitly. This difference leads to some auto-generated "onetime" schedule appeared in the configuration text file.

- FortiGate time schedule configuration cannot support "24:00" (equal to the next day's 00:00), when convert SonicWall recur time schedule like "M 00:00 to 24:00", we need to set the end time with "00:00". For FortiGate recur time schedule, "00:00" equals to "24:00", so it's just a display problem.

Local User and User Group:

- Because we cannot convert local user's cipher password string, so we set the users initiated password "123456".
- Nested user group is not supported. For example, there are two groups with the name group1 and group2, group1 belong to group2. SonicWall user group can support this nested group configuration, but FortiGate's user group cannot support this feature. By deault, we remove the nested configuration.

Route configuration:

- We don't support tunnel route now (static route with the next hop tunnel interface), because the whole VPN configuration is not supported within this version, not to mention tunnel interface objects.
- Auto generated routes like connected route and host route are also not converted.

NAT policy configuration:

- NAT policy configuration constraint.
  - Because FortiGate configure NAT rules within policy module, each SonciWall NAT rule will be auto generated to one policy entry. If the NAT status is enabled, then the policy status also set to enabled, and vice versa. NAT generated policies ID starts from 10001. Normal policy rules starts from 0.
  - For source NAT, we will create a new IP pool object for FortiGate policy's source address.

    For example, SonicWall source NAT policy like below.

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
All Interface IP	X2 IP	Any	Original	Any	Original

  After converting to FortiGate configuration, a new IP pool object with name "ippool_X2 IP" will be created, we just add a prefix "ippool_" before translated source address book "X2 IP".

  - For destination NAT, we will create a new VIP object for FortiGate policy's destination address.

-

  For example, SonicWALL's destination NAT policy like below.

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
LAN Subnets	Original	WoW Static IP	X0 IP	SSLVPN	Original

After converting to FortiGate configuration, a new VIP object with name "vip_X0 IP" will be created, we just add a prefix "vip_" before translated destination address book "X0 IP".

If destination NAT only remapped port number, then the translated destination address would be "original". In this case, the new create VIP object will refer to the translated service object's name.

- There is a constraint for destination NAT configuration, FortiGate destination NAT only support VIP and VIP group. FortiGate VIP object requires strict 1-to-1 map between the external IP/Port and the mapped IP/Port. But as I know, SonicWall doesn't have this constraint for destination NAT.

  For example, SonicWall source and destination NAT policy like below.

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
test_1112_grp	test_11_gw	test_12_gw	test_1211_grp	Echo	Original

This policy will translate IP packet's destination address, from address book "test_12_gw" to address group "test_1211_grp". Address book "test_12_gw" only contain one IP address, but address group "test_1211_grp" contain two address members "test_11_gw" and "test_12_gw". The result is we can't convert this NAT policy configuration to FortiGate policy configuration. This NAT policy will be ignored by converter because we don't know how to translate it.

- Another case:

Org Src	Tran Src	Org Dest	Tran Dest	Org Serv	Tran Serv
test_11_gw	test_12_gw	test_1112_grp	test_1211_grp	Echo	Original

This policy will translate IP packet's destination address, from address group "test_1112_grp" to address group "test_1211_grp". Assume that the address group "test_1112_grp" contains only one member "test_11_host", address group "test_1211_grp" contains two address members "test_11_gw" and "test_12_gw", then the problem is we cannot generate VIP objects correctly because of the VIP mapping constraint.

VIP mapping should be like this:

Ext ip mapped ip

Test_1112_grp Test_1211_grp

One IP address: Two IP address:

2.2.2.2 and 3.3.3.3

We cannot generate this VIP mapping object, because the "ext ip" and the "mapped ip" is not 1-to-1 mapping.

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 1: Resolved issues

Bug ID	Description
0206921	Fixed indenting bug when parsing Cisco/Juniper's command lines. Introduced mapping table for all supported commands and its sub-view commands.
0206922	Fixed bug when parsing Cisco's `time-range` command.
0200717	Improved converted object formatting.
0195987	Fixed bug when converting comments from Cisco to FortiGate.
0129690	Fixed bug when parsing RADIUS keyword in Check Point configurations.
0111946	Fixed bug when parsing host address types in firewall definitions for Check Point.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Table 2: Known issues

Bug ID	Description
0213185	Intermittent memory leak can occur with a parser failure. “System Out Of Memory” error appears. You must restart the software.
0212678	Errors parsing Cisco PIX access list..
0212680	Cisco IPSec VPN SA lifetime settings and transform-set translation error.
0212681	On Cisco PIX, one interface can refer to multiple `access-group` configurations.
0212683	Cisco VPN configurations can cause errors.
0212682	FortiConverter does not support Cisco ASA configurations with the new command keyword `object` .

Image checksums

To verify the integrity of the downloaded file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, go to *Download* > *Firmware Image Checksums*. In the *File Name* field, enter the firmware image's file name including its file extension, then click *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool